

Standartinė Android telefono apsauga

Deividas Ambrazevičius Nov 9, 2025

ambrazevicius.com

Įžanga

Šiandien mūsų telefonai žino daugiau apie mus nei bet kuris kitas įrenginys. Juose saugomi mūsų pokalbiai, nuotraukos, dokumentai, banko duomenys, sveikatos informacija ir net Jūsų lokacija. Dėl to telefonas tampa ne tik patogumo, bet ir potencialios rizikos šaltiniu.

Dauguma žmonių mano, kad jei nieko blogo nedaroma arba "Kam aš čia reikalinga tokia maža žuvis", jiems nereikia rūpintis privatumu - deja, tai mitas, nes net ir zvejams lengviau pagauti kelias mažas žuvis ir bendrojo sumo gaunasi didesnis "pelnas" nei pagaunant vieną didelę žuvį. Privatumas nėra nusikaltėlių privilegija, tai pagrindinė kiekvieno žmogaus teisė, apsauganti nuo neteisėto sekimo, duomenų nutekėjimo ir tapatybės vagysčių.

Šis gidas skirtas kiekvienam, net jei nesate pažengęs technologijų vartotojas. Visi žingsniai paaiškinti paprastai be techninių terminų, kad galėtumėte:

- apsaugoti save,
- padėti tėvams, vaikams ar seneliams,
- ir užtikrinti, kad jūsų "Android" įrenginys būtų saugesnis ir privatesnis.

Pradėkime

Nepriklausomai nuo to, koks yra tavo konkretus saugumo planas, kiekvienas turėtų peržiūrėti šiuos nustatymus savo telefone, kad padidintų privatumą ir saugumą.

Įjunkite dviejų veiksmų autentifikavimą savo "Google" paskyroje

Jei "Android" telefoną turite jau seniai, tikėtina, kad jau įjungėte dviejų veiksmų autentifikavimą (2FA), tai būdas apsaugoti savo internetines paskyras, reikalaujant papildomo patvirtinimo, jog tikrai jūs bandote prisijungti, be jūsų slaptažodžio. Tai reiškia, kad net jei kas

nors žino jūsų slaptažodį, jis vis tiek negalėtų prisijungti prie jūsų "Google" paskyros be antrojo autentifikavimo veiksnio.

Ką daryti?

Nors "Google" vis labiau reikalauja dviejų veiksmų autentifikavimo visoms paskyroms, naują paskyrą vis dar galima sukurti be jo. Jei nesate tikri, ar šią funkciją įjungėte, verta tai patikrinti. Tai galima padaryti bet kuriame įrenginyje, kuriame esate prisijungę prie savo paskyros.

Štai kaip tai padaryti:

1. **Nustatymai (Settings)** (kai kuriose versijose gali reikėti slinkti žemyn ir pasirinkti **Google Account**) → spustelėkite savo profilio nuotrauką → pasirinkite **Manage Your Google Account**.
2. Viršuje eikite į **Security** skiltį. Slinkite žemyn iki **Authenticator** arba **2-Step Verification phones**, kad įjungtumėte dviejų veiksmų autentifikavimą naudodami programėlę (rekomenduojama Google Authenticator) arba telefono numerį.
3. Iš čia taip pat galite sukurti **Passkey (slaptažodžio raktą)** savo paskyrai. Tai naujas būdas prisijungti, nereikalaujantis nei slaptažodžio, nei kodo, o vietoje to naudojamas jūsų įrenginio patvirtinimas. Norėdami jį sukurti, pasirinkite **Passkeys and security keys** → **Create a Passkey** ir vykdykite nurodymus.

 Jei esate padidintos rizikos vartotojas (pavyzdžiui, aktyvistas, žurnalistas ar politinės kampanijos dalyvis), apsvarstykite galimybę naudoti **saugumo raktą (security key)**. Jis labai atsparus sukčiavimui, tačiau praradus jį galite prarasti prieigą prie paskyros.

Dar vienas būdas papildomai apsaugoti paskyrą **Google Advanced Account Protection Program (išplėstinė paskyros apsauga)**. Ji rekomenduojama rizikos grupėms. Įjungus ją, aktyvuojamos papildomos funkcijos: pavojingų failų atsisiuntimo blokavimas "Chrome" naršyklėje, programų prieigos prie asmeninės informacijos ribojimas ir geresnė apsauga nuo sukčiavimo. Norint ją įjungti, reikia naudoti "passkey" arba fizinį saugumo raktą. Tai galima padaryti ir telefone.

Patikrinkite savo privatumo leidimus

Beveik kiekviena programėlė, kurią įdiegiate, prašo leidimų ir prieigos prie jūsų duomenų ar įrenginio funkcijų. Kartais tai logiška (pvz., kamera nori naudoti fotoaparata), bet dažnai programos prašo daugiau nei reikia.

Dėl to verta kartais peržiūrėti visus leidimus ir išjungti tuos, kurių nebenaudojate. Prieš tai taip pat pravartu ištrinti nenaudojamas programėles – tai supaprastins procesą ir sumažins riziką.

Ką daryti

Atidarykite **Settings → Security & Privacy → Privacy Controls → Permission manager**.

Čia pamatysite įvairius leidimus ir kiek programų turi prieigą prie kiekvieno iš jų. Eikite per kiekvieną kategoriją ir, jei matote, kad leidimas nereikalingas atšaukite jį. Jei dėl to programėlė nustos veikti, vėliau visada galite jį vėl įjungti.

Pagrindiniai leidimai, į kuriuos reikia atkreipti dėmesį:

1. Vietovės paslaugos (Location Services)

Patikrinkite, kurios programos gali matyti jūsų buvimo vietą. Galite pasirinkti:

- **Don't allow (Neleisti)** – programa negaus vietos duomenų.
- **Ask every time (Klausti kiekvieną kartą)** – programa paprašys leidimo kaskart.
- **Allow only while using (Leisti tik naudojant programą)** – prieiga tik kai ji atidaryta.
- **Always (Visada)** – prieiga visą laiką.

Taip pat galite pasirinkti, ar programa matys tikslią ar apytikslę vietą.

2. Kontaktai (Contacts)

Leidžia arba neleisti prieigos prie jūsų kontaktų sąrašo.

3. Nuotraukos ir vaizdo įrašai (Photos and videos)

Pasirinkimai:

- **Always allow all (Leisti viską)**
- **Allow limited access (Ribota prieiga)** – pasirinkite konkrečias nuotraukas.
- **Don't allow (Neleisti)**

4. Kamera (Camera)

Jei programa turi prieigą prie kameros be aiškos priežasties – išjunkite ją.

5. Mikrofonas (Microphone)

Tik programoms, kurioms iš tiesų reikia balso ar vaizdo įrašymo. Jei matote keistą programą – atjunkite prieigą.

Be to, jei ilgai nenaudosite programos, "Android" automatiškai atstatys jos leidimus į numatytuosius.

Išjunkite duomenų rinkimus reklamom

Reklamos identifikatorius ("AAID") leidžia trečiosioms šalims jus sekti. Jo išjungimas apsunkina reklamos tinklų ir duomenų brokerių galimybes jus profiluoti ir rinkti asmeninius duomenis.

Ką daryti

Norėdami jį išjungti:

1. Eikite į **Settings → Security & privacy → Privacy controls → Ads**
2. Pasirinkite **Delete advertising ID (Ištrinti reklamos ID)**.

Ijunkite "Find My Device" ir "Theft Protection" funkcijas

"Find My Device" leidžia rasti jūsų telefoną, jei jis pamestas ar pavogtas. Jei tikėtina, kad telefono neatgausite, galite jį nuotoliniu būdu ištrinti.

"Find My Device" naudoja vietovės duomenis (Wi-Fi, mobilųjį tinklą, "Bluetooth") tam, kad surastų įrenginį. "Google" teigia, kad ši informacija yra šifruota ir matoma tik jums. Visgi visada yra tam tikra rizika, kad duomenys gali būti panaudoti ne pagal paskirtį.

Ką daryti

1. Eikite į **Settings → Security & privacy → Device Finders → Find My Device** ir įjunkite **Use Find My Device**.
2. Galite įjungti **Remote Lock**: leisite užrakinti įrenginį nuotoliniu būdu naudodami telefono numerį.
3. Apsvarstykite **Theft Protection (Apsaugą nuo vagystės)**. Ji naudoja įrenginio jutiklius ir signalus, kad aptiktų, jei kas nors jį griebia ir bėga. Jei tai įvyksta, ekranas automatiškai užsirakina.
 - Eikite į **Settings → Security & privacy → Device Unlock → Theft Protection** ir įjunkite **Theft Detection Lock** bei **Offline Device Lock**.
4. Taip pat galite įjungti **Identity Check**, kuris reikalauja biometrinio patvirtinimo prieš keičiant svarbius nustatymus (pvz., "Factory Reset" ar "Find My Device" išjungimą). Ši funkcija prieinama ne visuose telefonuose.

Atlikite "Google" privatumo patikrą ("Privacy Checkup")

Kadangi tikriausiai naudojate "Google" paskyrą ir kompiuteryje, ir telefone, daug svarbių privatumo nustatymų yra ne telefone, o jūsų paskyros puslapyje. Todėl verta atlikti "**Privacy Checkup**", kad įsitikintumėte, jog netyčia nebendrintumėte duomenų, tokių kaip "YouTube" istorija ar buvimo vieta.

Ką daryti

1. Telefone atidarykite **Settings** → **Google Account** → profilio piktogramą.
2. Pasirinkite **Review your privacy settings** (arba **Manage Your Google Account** → **Privacy suggestions available**).
3. Taip pat galite tiesiogiai apsilankyti „Privacy Checkup“ puslapyje naršyklėje, jei esate prisijungę prie savo paskyros.
4. Peržiūrėkite kiekvieną puslapį ir įsitikinkite, kad neleidžiate rinkti ar dalintis duomenimis, kurių nenorite.

Nuspręskite, kaip norite tvarkyti atsargines kopijas

Atsarginės kopijos tai labai svarbus būdas apsaugoti jūsų duomenis, jei netyčia pamestumėte telefoną arba jis sugestų. Jos taip pat praverčia, kai patys išvalote telefoną, pavyzdžiui, įsigiję naują įrenginį arba ruošdamiesi situacijai, kurioje nenorite turėti jokių asmeninių duomenų.

Turint naujausią atsarginę kopiją, telefoną galima greitai atkurti ir nereikia rankiniu būdu vėl atsisiųsti programėlių ir duomenų.

Ką daryti?

"Android" leidžia šiek tiek pritaikyti, kaip kuriami atsarginiai duomenų kopijavimai, bet pasirinkimų nėra daug.

1. Atidarykite **Nustatymai (Settings)** > **Sistema (System)** > **Atsarginė kopija (Backup)**.
2. Čia galite pasirinkti automatiškai kurti atsargines kopijas tik nuotraukoms ir vaizdo įrašams arba visiems kitiems duomenims.
 - Prisiminkite: dalis šių duomenų bus užšifruota pagal jūsų įrenginio atrakinimo kodą, bet ne viskas.

Jei nenorite naudoti "Google" debesų, galite kurti vietinę atsarginę kopiją kompiuteryje:

- **Windows naudotojai** gali naudoti programą **Google Quick Share**, kad duomenis perkeltų belaidžiu būdu, arba tiesiog prijungti telefoną prie kompiuterio **USB laidu** ir

pasirinkti Failų perdavimas (File Transfer). Atsidarius langui, pertempkite norimus failus į kompiuterį.

- **Mac naudotojams** šiuo metu nėra paprasto ir nemokamo būdo sukurti rankinę atsarginę kopiją, tačiau verta pasitikrinti oficialią „Google“ pagalbos svetainę – gal yra naujų sprendimų.

Jei ketinate parduoti ar atiduoti savo Android telefoną, arba tiesiog norite jį išvalyti, atlikite gamykloje nustatymų atkūrimą (factory reset) pagal Google instrukcijas (jos gali skirtis priklausomai nuo gamintojo).

Kai vėl prisijungsite prie telefono su ta pačia „Google“ paskyra, kurioje saugojote atsarginę kopiją, sekite ekrane pateiktas instrukcijas ir atkurtas bus visos turinys.

Įjunkite išplėstinę apsaugą

„Advanced Protection“ tai Google išplėstinės apsaugos programos dalis, kuri padeda apsaugoti jūsų paskyrą nuo apgaulingų (phishing) laiškų ir kenksmingų atsisiuntimų. Kai ši funkcija įjungta „Android“ telefone, ji sustiprina saugumą, nes:

- įjungia kai kurias papildomas apsaugos funkcijas, kurios įprastai būna išjungtos,
- neleidžia išjungti tų funkcijų, kurios pagal numatymą įjungtos,
- prideda naujų saugumo priemonių.

Visa tai kartu padeda geriau apsaugoti jūsų duomenis, sumažina riziką patekti į nesaugias svetaines ar bendrauti su nepažįstamais žmonėmis internete.

Ką daryti?

„Advanced Protection“ galima lengvai įjungti ar išjungti, todėl verta pabandyti.

Vis dėlto atminkite, kad ši funkcija gali pakeisti jūsų įprastą telefono naudojimą.

Pavyzdžiui:

- ji **išjungia „JavaScript“ optimizavimą „Chrome“ naršyklėje**, todėl kai kurios svetainės gali veikti netinkamai;
- **užblokuojamas nežinomų programėlių diegimas**;
- **apsaugos nuo sukčių funkcijos** gali kartais klaidingai atpažinti teisėtus skambučius kaip įtartinus.

Šiuo metu "Advanced Protection" prieinama tik telefonams, kuriuose veikia **Android 16** versija. Jei jūsų įrenginys jos nepalaiko, šios parinktys dar nematysite.

Įjungimo žingsniai:

1. Atidarykite programą **Nustatymai (Settings)**.
2. Pasirinkite **Sauga ir privatumas (Security and Privacy) > Advanced Protection**.
3. Įjunkite parinktį šalia „Įrenginio apsauga“ (**Device Protection**).

Sukurkite privačią erdvę

Jei norite paslėpti jautrias ar asmenines programėles, "Private Space" funkcija yra paprasčiausias būdas tai padaryti.

Sukūrus privačią erdvę:

- gaunate **atskirą programėlių rinkinį**,
- galite (jei norite) **prijungti kitą „Google“ paskyrą**,
- visų tų programėlių duomenys bus **visiškai atskirti nuo likusio telefono turinio**.

Tai naudinga, jei norite pasilikti kai kurią informaciją tik sau – pavyzdžiui:

- naudotis **šifruotomis susirašinėjimo programėlėmis**,
- turėti **atskirą nuotraukų biblioteką**,
- arba laikyti programėles, kurios nėra itin privačios, bet jums jų kartais reikia – pvz., **žemėlapių** ar **pavežėjimo** programėles.

Ką daryti?

1. Atidarykite **Nustatymai (Settings) > Saugumas ir privatumas (Security & privacy) > Private space**.
2. Sekite ekrane pateiktas instrukcijas, kad sukurtumėte naują erdvę.
 - Galite pasirinkti naudoti **atskirą PIN kodą** arba tą patį, kuriuo atrakinate telefoną.
3. Kai būsite paraginti, galite **susikurti naują „Google“ paskyrą**.
 - Tai neprivaloma, bet naudinga, jei nenorite, kad privatūs duomenys (naršymo istorija, nuotraukos ir kt.) būtų automatiškai sinchronizuojami su jūsų pagrindine paskyra.
4. Kai viską nustatysite, **privačios erdvės programėlės** bus matomos **programėlių sąrašo apačioje**.

Išjunkite 2G ryšį

Kai kurios organizacijos, įskaitant teisėsaugą ar vyriausybines tarnybas, gali naudoti specialius įrenginius, vadinamus IMSI gaudyklėmis.

Šie įrenginiai gali:

- sekti jūsų telefono buvimo vietą,
- perimti ar trikdyti ryšį,
- bandyti įsilaužti į telefoną ir įdiegti kenkėjišką programinę įrangą,
- siųsti šlamštą ar sukčiavimo žinutes.

Tokie įrenginiai dažnai apsimeta 2G mobiliojo ryšio stotimis, kad apgautų jūsų telefoną ir priverstų jį prisijungti prie netikro tinklo.

Kad apsisaugotumėte nuo tokių apgaulių, galite išjungti 2G ryšio palaikymą savo telefone. Nors nėra daug įrodymų, kad tokie įrenginiai būtų plačiai naudojami prieš paprastus žmones, šį žingsnį verta atlikti, nes jis paprastas, saugus ir neturi įtakos kasdieniam telefono naudojimui.

Ką daryti

Priklausomai nuo telefono gamintojo, "Android" versijos ir jūsų mobiliojo tinklo operatoriaus, galite turėti vieną arba kelias apsaugos parinktis:

- **išjungti 2G ryšį,**
- **reikalauti šifruoto (saugaus) ryšio.**

Štai kaip tai padaryti:

1. Atidarykite **Nustatymai (Settings) > Tinklas ir internetas (Network & Internet) > SIM kortelės (SIMs).**
2. Pasirinkite savo **mobiliojo tinklo operatorių.**
3. Suraskite parinktį „**Leisti 2G**“ (**Allow 2G**) ir **išjunkite ją**, kad visiškai išjungtumėte 2G ryšį.
4. Jei matote parinktį „**Reikalauti šifruoto ryšio**“ (**Require Encryption**), **įjunkite ją**, kad telefonas niekada nenaudotų nesaugaus (nešifruoto) ryšio prisijungdamas prie bazinės stoties.

Papildomi patarimai

Ne visiems žmonėms reikia tų pačių nustatymų, kai kuriuos "Android" pakeitimus atlikti lengviau nei kitus.

Toliau pateikiami keli papildomi žingsniai, kuriuos galite apsvarstyti, priklausomai nuo savo poreikių:

Išjunkite galimybę jungtis prie WEP tinklų

Kodėl tai svarbu?

WEP - tai senas "Wi-Fi" tinklo apsaugos protokolas, turintis daug saugumo spragų.

Dauguma šiuolaikinių tinklų jo jau nenaudoja, tačiau vis dar galima sutikti senų WEP tinklų, prie kurių jungtis nerekomenduojama, nes jie lengvai pažeidžiami.

Nuo "**Android 15**" versijos atsirado galimybė visiškai išjungti WEP tinklų palaikymą, kad telefonas niekada neprisijungtų prie nesaugaus tinklo.

Ši funkcija **nepasiekiamo senesniuose įrenginiuose**.

Ką daryti?

1. Atidarykite **Nustatymai (Settings) > Tinklas ir internetas (Network & Internet) > Internetas (Internet)**.
2. Slinkite žemyn iki **Tinklo nuostatų (Network preferences)**.
3. Išjunkite parinktį „**Leisti WEP tinklus**“ (**Allow WEP networks**).

Pabaigai

Privatumas telefone nėra prabanga ar sudėtinga technologija tai maži įpročiai, kurie ilgainiui tampa jūsų saugumo dalimi.

Vos keli nustatymai gali:

- Apsaugoti jus nuo duomenų nutekėjimo,
- Neleisti reklamos tinklams sekti jūsų veiklos,
- Ir padėti rasti ar užrakinti telefoną, jei jis pamestas ar pavogtas.

Svarbiausia, skirkite tam kelias minutes dabar, kol viskas gerai. Tokiu būdu užkirsite kelią problemoms ateityje.

Jei šie žingsniai atrodo sudėtingi vyresniems - padėkite jiems, o ypač tiems, kurie nesidomi technologijomis, bet kasdien naudoja telefoną.

Rūpindamiesi savo skaitmeniniu saugumu, jūs saugote ne tik duomenis, bet ir savo asmeninę erdvę bei laisvę.

Ryšio kontrolei egzistuoja ir specialūs sprendimai, pasyvūs (pvz., ekranavimo/"Faraday" dėklai), programiniai "no-radio" profiliai bei įrangos jungikliai, leidžiantys fiziškai ar programiškai apriboti įrenginio skleidžiamus signalus. **Atkreipiu dėmesį**, kad aktyvūs radijo ryšio slopintuvai ("jammers") daugelyje šalių yra draudžiami, naudokite tik teisėtus metodus ir laikykitės galiojančių įstatymų.

Jei norite eiti toliau nei standartiniai nustatymai, parašykite, paruošiu konkretų planą, pakonsultuosiu, sukomplektuosiu įrankius ir įrenginį pagal jūsų grėsmių modelį bei poreikius. (Signal: **davidamber.28**)